JOURNAL OF NUMBER THEORY 9, 321–329 (1977)

Sums of Roots of Unity in Cyclotomic Fields

EDWARD H. GROSSMAN

Department of Mathematics, City College of CUNY, New York, New York 10031

Communicated by N. Ankeny

Received January 4, 1975; revised September 8, 1975

Let ζ_n denote a primitive nth root of unity, $n \geqslant 4$. For any integer k, $2 \leqslant k \leqslant n-2$ it is shown that the diophantine equation $1 + \zeta_n + \cdots + \zeta_n^{k-1} = \rho\alpha^q$ has no solutions with ρ, α in $\mathbb{Q}(\zeta_n)$, ρ a root of unity, α an algebraic integer, and q an integer $\geqslant 2$, except when $n = 10$, 12, or 30, where the solutions are completely determined.

1. INTRODUCTION

Let ζ_n denote a primitive nth root of unity. In this paper we present a proof of a generalization of a theorem of Ennola.

THEOREM. *Let $n \geqslant 4$, $2 \leqslant k \leqslant n-2$, and $q \geqslant 2$. Then the equation*

$$1 + \zeta_n + \cdots + \zeta_n^{k-1} = \rho\alpha^q, \tag{1}$$

where ρ, α are in $\mathbb{Q}(\zeta_n)$, ρ a root of unity and α an algebraic integer, has no solutions except

$n = 10, \quad k = 3, \quad \rho = -\zeta_{10}^{-2v}, \quad \alpha = \zeta_{10}^{v+2}(1 + \zeta_{10}^2), \quad q = 2;$

$n = 10, \quad k = 7, \quad \rho = -\zeta_{10}^{-2v}, \quad \alpha = \zeta_{10}^{v-2}(1 + \zeta_{10}^2), \quad q = 2;$

$n = 12, \quad k = 5, \quad \rho = \zeta_{12}^{-2v+1}, \quad \alpha = \zeta_{12}^{v}(1 + \zeta_{12}), \quad q = 2;$

$n = 12, \quad k = 7, \quad \rho = \zeta_{12}^{-2v}, \quad \alpha = \zeta_{12}^{v+2}(1 + \zeta_{12}), \quad q = 2;$

$n = 30, \quad k = 11, \quad \rho = -\zeta_{30}^{-2v}, \quad \alpha = \zeta_{30}^{v+9}(1 + \zeta_{30} + \zeta_{30}^2), \quad q = 2;$

$n = 30, \quad k = 19, \quad \rho = -\zeta_{30}^{-2v}, \quad \alpha = \zeta_{30}^{v+11}(1 + \zeta_{30} + \zeta_{30}^2), \quad q = 2;$

where v is any integer.

Using more complicated methods than ours, Ennola [1, 2] has analyzed (1) completely when $\rho = 1$, and special cases had been previously investigated

ISSN 0022-314X

by Mordell [3] and Newman [4, 5]. Some of our techniques are derived from the latter's work.

It will be convenient throughout the paper to denote ζ_n simply by ζ when n is understood. Also we let

$$\eta_k = 1 + \zeta + \cdots + \zeta^{k-1} = (1 - \zeta^k)/(1 - \zeta).$$

As an immediate consequence of the above result and Dirichlet's unit theorem we note the following corollary.

COROLLARY. *If $n \geqslant 4$ and η_k, $2 \leqslant k \leqslant n - 2$, is a unit, (in particular if $(k, n) = 1$) then it is part of a system of fundamental units of $\mathbb{Q}(\zeta)$ with the exceptions $n = 10, 12,$ and 30 where for $n = 10$, $(-\eta_3)^{1/2}$, $(-\eta_7)^{1/2}$; for $n = 12$, $(\zeta_{12}\eta_5)^{1/2}$, $\eta_7^{1/2}$; and for $n = 30$, $(-\eta_{11})^{1/2}$, $(-\eta_{19})^{1/2}$ have this property.*

The proof of the Theorem proceeds by assuming for given ζ_n, k, and q the existence of solutions ρ and α to (1) and deducing a contradiction except in the stated cases. Note then that since $|\eta_k| \neq 0, 1$ we may assume in what follows that α is neither zero nor a root of unity.

Before commencing the proof we recall that $\mathbb{Q}(\zeta)$ is an abelian extension of $\mathbb{Q}$ with Galois group given by the substitutions $\zeta \to \zeta^v$, $(v, n) = 1$. If α is a unit in $\mathbb{Q}(\zeta)$ then $\bar{\alpha} = \rho\alpha$, where ρ is a root of unity of $\mathbb{Q}(\zeta)$ and $\bar{\alpha}$ denotes the complex conjugate of α. Finally, letting N denote the norm map from $\mathbb{Q}(\zeta_n)$ to $\mathbb{Q}$ we will make repeated use of the following formulas. For $n \geqslant 3$

$$N(1 - \zeta_n) = \begin{cases} p & \text{if } n = p^v, \\ 1 & \text{if } n \neq p^v, \end{cases} \qquad p \text{ a prime,} \tag{2}$$

and

$$N(1 + \zeta_n) = \begin{cases} p & \text{if } n = 2p^v, \\ 1 & \text{if } n \neq 2p^v, \end{cases} \qquad p \text{ a prime.} \tag{3}$$

2. Proofs

The main tool in the analysis of (1) is given in the first lemma.

LEMMA 1. *Let K be a normal extension of $\mathbb{Q}$ such that for all $\alpha \in K$ and all automorphisms σ of K into $\mathbb{C}$ $\sigma(\bar{\alpha}) = \overline{\sigma(\alpha)}$, where $\bar{\alpha}$ denotes the complex conjugate of α. If α is a nonzero algebraic integer of K, not a root of unity, and ρ, ξ are any roots of unity of K, then for $m > 2$, $\beta = \rho\alpha^m + \xi$ is never a unit. For $m = 2$, β is a unit only if $\rho\alpha^2 = \epsilon\xi$, where ϵ is totally real.*

Proof. Observe that if z is any complex number and $|\rho| = |\xi| = 1$, then for $m \geqslant 2$

$$|\rho z^m + \xi| \geqslant \max(|z|, 1)^{m-2} ||z|^2 - 1|.$$

Applying this inequality to the conjugates β_v of β, we find for the absolute norm of β

$$\begin{aligned} |N(\beta)| &\geqslant \prod \max(|\alpha_v|, 1)^{m-2} \prod ||\alpha_v|^2 - 1| \\ &= \prod \max(|\alpha_v|, 1)^{m-2} |N(|\alpha|^2 - 1)|, \end{aligned}$$

using the condition $\sigma(\bar{\alpha}) = \overline{\sigma(\alpha)}$. Since α is not a root of unity, $|\alpha|^2 - 1$ is a nonzero algebraic integer of K and $\prod \max(|\alpha_v|, 1) > 1$. If $m > 2$ this shows that β is never a unit and if $m = 2$, β is a unit only if for all conjugates

$$|\rho_v \alpha_v^2 + \xi_v| = ||\alpha_v|^2 - 1|,$$

and therefore $\rho_v \alpha_v^2 = \epsilon_v \xi_v$, where ϵ_v is totally real.

The proof of the theorem is split into several cases, depending on the power of two dividing n.

Case 1. If $\zeta = \zeta_n$, where $n > 3$ is odd and if $2 \leqslant k \leqslant n - 2$ then (1) has no solutions.

Proof. Since n is odd the map $\sigma : \zeta \to \zeta^2$ is an automorphism of $\mathbb{Q}(\zeta)$. Assuming for some k that (1) has a solution ρ_1, α_1 we apply σ and divide the result by (1) to obtain

$$(1 + \zeta^k)/(1 + \zeta) = \rho_2 \alpha_2^q.$$

Applying σ again yields

$$(1 + \zeta^{2k})/(1 + \zeta^2) = \rho_3 \alpha_3^q.$$

Then

$$\rho_3 \alpha_3^q + \zeta^{k-1} = (1 + \zeta^{k-1})(1 + \zeta^{k+1})/(1 + \zeta^2)$$

is a unit by virtue of (3) and the condition $k \not\equiv \pm 1 \pmod{n}$. By Lemma 1 this is impossible for $q \geqslant 3$.

If $q = 2$ and (1) has a solution we may assume since n is odd that $\eta_k = \pm\alpha^2$. Since $\sigma(\alpha) \equiv \alpha^2 \pmod{2}$ we have

$$\frac{1 - \zeta^{2k}}{1 - \zeta^2} = \pm\sigma(\alpha)^2 \equiv \pm\left(\frac{1 - \zeta^k}{1 - \zeta}\right)^2 \pmod{4}$$

and this implies that $1 - \zeta^{k\pm 1} \equiv 0 \pmod{2}$ which contradicts (2).

Case 2. If $\zeta = \zeta_n$, where $n = 2m$, $m \geqslant 3$ odd, and if $2 \leqslant k \leqslant n - 2$, then (1) has no solutions except for $n = 10$ or 30.

Proof. We have $\zeta = -\lambda$, where λ is a primitive mth root of unity. If k is even and (1) has a solution then

$$\eta_k = (1 - \lambda^k)/(1 + \lambda) = \rho\alpha^q.$$

From (3) either $\rho\alpha^q + \lambda^{k-1}$ or $\rho\alpha^q + \lambda^k$ is a unit. This is not possible for $q \geqslant 3$ and if $q = 2$ Lemma 1 implies that $\eta_k = \epsilon\lambda^{k-1}$ or $\eta_k = \epsilon\lambda^k$, where ϵ is real. Comparing complex conjugates yields a contradiction.

If k is odd the $\eta_k = (1 + \lambda^k)/(1 + \lambda)$. If (1) has a solution, applying the automorphism $\sigma : \lambda \to \lambda^2$ as in Case 1 leads to a contradiction if $q \geqslant 3$. If $q = 2$ we may write (1) in the form $\eta_k = \pm\alpha^2$.

If $\eta_k = \alpha^2$ then using that $\sigma(\alpha) \equiv \alpha^2 \pmod 2$ gives

$$(1 + \lambda^{2k})/(1 + \lambda^2) \equiv [(1 + \lambda^k)/(1 + \lambda)]^2 \qquad (\text{mod } 4),$$

hence

$$(1 - \lambda^{k-1})(1 - \lambda^{k+1}) \equiv 0 \qquad (\text{mod } 2).$$

By (2) this can only happen if $k \equiv \pm 1 \pmod m$ which since $k < 2m$ implies $k = m \pm 1 \equiv 0 \pmod 2$, a contradiction.

Suppose next that $\eta_k = -\alpha^2$. If $\eta_k - 1$ or $\eta_k - \lambda^k$ is a unit then Lemma 1 implies that for a totally real ϵ, $\eta_k = \epsilon$ or $\eta_k = \epsilon\lambda^k$. Since $\overline{\eta_k} = \lambda^{1-k}\eta_k$ this is impossible. Using (2) it is easy to see that $\eta_k - 1$ and $\eta_k - \lambda^k$ are not units only when λ^{k-1} and λ^{k+1} are roots of unity of odd prime power orders.

If m is divisible by at least two primes then these orders are of the form p^a and q^b for distinct odd primes p and q and $m = p^a q^b$. If $m = p^c$ then the orders of λ^{k-1} and λ^{k+1} are of the form p^a, p^b where $\max(a, b) = c$. Note in this case that from the equations $\eta_k - 1 = -\alpha^2 - 1$ and $\eta_k - \lambda^k = -\alpha^2 - \lambda^k$ it follows that -1 is a quadratic residue mod p and so $p \equiv 1 \pmod 4$. In both cases, applying the automorphism σ as above gives

$$1 + \lambda + \lambda^2 + \lambda^k + \lambda^{k+2} + \lambda^{2k} + \lambda^{2k+1} + \lambda^{2k+2} \equiv 0 \quad (\text{mod } 2). \quad (4)$$

If m is not a prime power, letting $\xi = \lambda^{(k-1)/2}$ and $\rho = \lambda^{(k+1)/2}$ this may be written as

$$\rho^2 + (\rho + \rho^3)\,\xi + (1 + \rho^4)\,\xi^2 + (\rho + \rho^3)\,\xi^3 + \rho^2\xi^4 \equiv 0 \quad (\text{mod } 2). \qquad (5)$$

Since the ring of integers in $\mathbb{Q}(\xi, \rho)$ is a free module over the integers of $\mathbb{Q}(\rho)$ with basis $\{1, \xi, \ldots, \xi^n\}$, $h = \varphi(p^a) - 1$, (5) implies that when $h \geqslant 4$ all coefficients are divisible by 2 in $\mathbb{Q}(\rho)$, which is impossible. By interchanging the roles of ξ and ρ we see that the only remaining case is when the pair ξ and ρ are 3rd and 5th roots of unity. Then $m = 15$ and we obtain mod 30 the odd values $k = 11$ and 19, in which cases the stated solutions for α may be found by direct but somewhat lengthy computation.

If $m = p^c$ is a prime power then for every integral j we have

$$\lambda^j = \sum_{i=0}^{h} a_{ij}\lambda^i, \qquad h = \varphi(p^c) - 1$$

and $a_{0j} \equiv 1 \pmod 2$ only for $j \equiv 0, -p^{c-1} \pmod{p^c}$. Therefore in order for (4) to hold at least one of k, $k + 2$, $2k$, $2k + 1$, or $2k + 2$ must satisfy one of the latter congruences. Using the condition $p \equiv 1 \pmod 4$ noted above to facilitate the examination of these cases one finds that (4) holds only for $m = 5$ and $k \equiv 2$ or $3 \pmod 5$. From this it is any easy matter to find the solutions given in the statement of the theorem. This completes the analysis of Case 2.

Case 3. If $n \equiv 0 \pmod 4$ and $n > 4$ then (1) has no solutions for $k = (n/2) \pm 1$ and q an odd prime.

Proof. It suffices to show that the equation

$$(1 + \zeta)/(1 - \zeta) = \rho\alpha^q \tag{6}$$

has no solutions. If α satisfies (6) then α is a unit so that $\bar{\alpha} = \zeta^r\alpha$. Comparing complex conjugates in (6) gives $-\rho = \rho^{-1}\zeta^{rq}$. Thus ρ^2 is a qth power and therefore so is ρ. Hence for a possibly new α we may assume that

$$(1 + \zeta)/(1 - \zeta) = \alpha^q. \tag{7}$$

If $q \mid n$ then writing $\alpha = \sum a_v\zeta^v$
we have

$$\alpha^q = q\gamma + \sum a_v\zeta^{qv} = q\gamma + \beta,$$

where β is in the proper subfield $\mathbb{Q}(\zeta^q)$ of $\mathbb{Q}(\zeta)$. Thus there is an $s \not\equiv 1 \pmod n$, $(s, n) = 1$, such that the automorphism σ defined by $\zeta \to \zeta^s$ fixes β. Applying σ to (7) gives

$$(1 + \zeta^s)/(1 - \zeta^s) \equiv (1 + \zeta)/(1 - \zeta) \qquad \pmod q,$$

which is impossible for $s \not\equiv 1$.

If $q \nmid n$ and α satisfies (7) then $\bar{\alpha} = \zeta^r\alpha$, where $\zeta^{rq} = -1$ and hence also $\zeta^r = -1$. From (7) we also have that

$$\alpha^q - 1 = 2\zeta/(1 - \zeta) \tag{8}$$

so that letting $\lambda = 1 - \zeta$, $\alpha^q \equiv 1 \pmod{2\lambda^{-1}}$. Let τ be the automorphism of $\mathbb{Q}(\zeta)$ defined by $\zeta \to -\zeta$. Then for any integral β, $\tau(\beta) \equiv \beta \pmod 2$. Note also that since α satisfies (7) $(\alpha\tau(\alpha))^q = 1$ which since $q \nmid n$ implies $\alpha\tau(\alpha) = 1$. Hence $\alpha^2 \equiv \alpha\tau(\alpha) \equiv 1 \pmod 2$ which combined with $\alpha^q \equiv 1 \pmod{2\lambda^{-1}}$ implies $\alpha \equiv 1 \pmod{2\lambda^{-1}}$. From (8) then we obtain

$$\alpha - 1 = 2\gamma\lambda^{-1}, \tag{9}$$

where γ is a unit with $\bar{\gamma} = \zeta^{s-1}\gamma$.

Taking the complex conjugate of (9) and eliminating γ gives

$$-(1 - \zeta^s)\,\alpha = \zeta^s + 1$$

and therefore

$$-(1 - \zeta^{sq})(1 + \zeta) \equiv (1 - \zeta)(\zeta^{sq} + 1) \qquad (\mathrm{mod}\ q),$$

which implies using the norm formula (2) that $sq + 1 \equiv 0 \pmod n$ so that in particular $(s, n) = 1$. Hence we have

$$\alpha = (\zeta^s + 1)/(\zeta^s - 1).$$

Letting σ denote the automorphism taking $\zeta \to \zeta^s$ we obtain from (7) that $\sigma(\alpha) = \alpha_2$ satisfies

$$\alpha_2{}^q = (1 + \zeta^s)/(1 - \zeta^s),$$

and therefore

$$\alpha = -\alpha_2{}^q.$$

Letting $s = s_1$ and $\alpha = \alpha_1$ an obvious induction then shows that for any $j \geqslant 1$ there exist an s_j with $(s_j, n) = 1$ and a unit α_j such that

$$\alpha_j = (\zeta^{s_j} + 1)/(\zeta^{s_j} - 1) \qquad \text{and} \qquad \alpha_{j+1}^q = -\alpha_j\,.$$

It follows then that for every $j \geqslant 1$ there exists a β_j with

$$(1 + \zeta)/(1 - \zeta) = \beta_j^{q^j},$$

which is possible only if $(1 + \zeta)/(1 - \zeta)$ is a root of unity. Since $n > 4$ this is not the case and the proof is complete.

Case 4. Let $\zeta = \zeta_n$, where $n = 2^v m$, m odd, and $v \geqslant 1$ if $m \geqslant 3$ and $v \geqslant 2$ if $m = 1$. Then (1) has no solutions with q an odd prime and $k \not\equiv 0$, $\pm 1 \pmod n$.

Proof. If k is even then for n a power of two $\eta_k - 1$ is a unit, and if n is divisible by an odd prime either $\eta_k - 1$ or $\eta_k + \zeta^k$ is a unit. In both cases then Lemma 1 gives the result.

For odd k we use induction on v, the initial cases being part of Case 2 or when $n = 4$ being vacuous. If $k \equiv (n/2) \pm 1 \pmod n$ then Case 3 applies.

Otherwise we assume (1) has a solution and apply the automorphism $\sigma\colon \zeta \to -\zeta$. Multiplying the results gives

$$(1 - \zeta^{2k})/(1 - \zeta^2) = \rho\sigma(\rho)(\alpha\sigma(\alpha))^q.$$

Since $\mathbb{Q}(\zeta^2)$ is the fixed field of σ, and ζ^2 has order $n/2$ the last equation contradicts the inductive hypothesis, thus proving this case.

Case 5. Let $\zeta = \zeta_n$ with $n \equiv 0 \pmod 4$. Then (1) has no solutions for any $q \geqslant 3$ and for $q = 2$ only those stated in the theorem for $n = 12$.

Proof. By Case 4 it suffices to show that (1) has no solutions for $q = 4$, and to exhibit the solutions for $q = 2$. Assume then that (1) has a solution with $q = 4$ or 2. Applying the automorphism $\sigma : \zeta \to - \zeta$ and using $\sigma(\alpha) \equiv \alpha \pmod 2$ gives

$$\frac{1 - (-1)^k \zeta^k}{1 + \zeta} \equiv \pm \left(\frac{1 - \zeta^k}{1 - \zeta}\right) \quad (\text{mod } 2q). \tag{10}$$

If k is even (10) implies that $1 - \zeta^k \equiv 0 \pmod q$. For $q = 4$ this is not possible and if $q = 2$ only for $k = n/2$. In that case $\eta_k = 2(1 - \zeta)^{-1}$ and therefore

$$\rho\alpha^2 - 1 = \eta_k - 1 \equiv (1 + \zeta)/(1 - \zeta)$$

is a unit. Lemma 1 implies that $\rho\alpha^2$ is real, which is clearly false.

If k is odd (10) implies that $1 - \zeta^{k\pm 1} \equiv 0 \pmod q$, which cannot occur unless $q = 2$ and $k = (n/2) \pm 1$. Therefore (1) has no solution if $q \geqslant 3$ and if $q = 2$ it suffices to consider the solution of

$$(1 + \zeta)/(1 - \zeta) = \alpha^2 \tag{11}$$

and

$$(1 + \zeta^{-1})/(1 - \zeta) = \beta^2. \tag{12}$$

If (11) holds then the norm formulas (2) and (3) imply that α is a unit so that $\bar{\alpha} = \zeta^a\alpha$, where $\zeta^{2a} = -1$. Also from (11)

$$\alpha^2 - 1 = (\alpha - 1)(\alpha + 1) = 2\zeta/(1 - \zeta). \tag{13}$$

If $\mathfrak{p}$ is any prime ideal dividing (2) in $\mathbb{Q}(\zeta)$ then (13) implies that $\text{ord}_{\mathfrak{p}}(\alpha - 1) = \text{ord}_{\mathfrak{p}}(\alpha + 1)$. If $n = 2^v$ then $\mathfrak{p} = (1 - \zeta)$ is such an ideal so that (13) implies $\text{ord}_{\mathfrak{p}}(2)$ is odd, which is false. For $n = 2^v m$, $m \geqslant 3$ odd $1 - \zeta$ is a unit so that (13) yields $(\alpha - 1)^2 = (2) = (1 + \zeta^a)^2$. Thus

$$\alpha - 1 = \epsilon(1 + \zeta^a), \tag{14}$$

where ϵ is a unit. Using $\bar{\epsilon} = \zeta^b\epsilon$, (14) yields on taking complex conjugates

$$\alpha = (1 - \zeta^{b-a})/(\zeta^a - \zeta^{b-a}).$$

Using this expression for α in (11) and recalling that $\zeta^{2a} = -1$ gives

$$1 - \zeta^{b-a}(1 + \zeta^{-a}) + \zeta^{b+1}(1 + \zeta^{-a}) + \zeta^{2b+1} = 0 \tag{15}$$

and therefore $(1 + \zeta^{-a}) | (1 + \zeta^{2b+1})$ which since $n \equiv 0 \pmod 4$ implies $\zeta^{2b+1} = \pm\zeta^{-a}$.

If $\zeta^{2b+1} = \zeta^{-a}$ we obtain from (15)

$$1 - \zeta^{b-a} + \zeta^{b+1} = 0 \tag{16}$$

and therefore $|1 + \zeta^{b+1}| = |1 - \zeta^{b-a}| = 1$. Hence ζ^{b+1} and $-\zeta^{b-a}$ are primitive third roots of unity and so is $-\zeta^{a+1}$. Therefore ζ is a 12th root of unity and we have $\zeta^a = \pm\zeta^3$, $\zeta^{b+1} = \zeta^{\pm 4}$, $\zeta^{b-a} = -\zeta^{\pm 4}$. An examination of these cases, using that $\zeta^4 - \zeta^2 + 1 = 0$, yields as the only solutions of (11) $\alpha = -\zeta(1 + \zeta)$.

If $\zeta^{2b+1} = -\zeta^{-a}$, (15) becomes

$$1 + \zeta^b + \zeta^{b+1-a} = 0$$

and again this implies ζ is a primitive 12th root of unity with $\alpha = \zeta(1 + \zeta)$ a solution to (11). Combining these results we obtain the family of solutions $\alpha = \zeta_{12}^{v+1}(1 + \zeta_{12})$ to (1). From the analysis of (11) we obtain by conjugation the solutions of

$$(1 + \zeta^{-1})/(1 - \zeta) = \zeta\alpha^2,$$

and hence the two families of solutions stated for $n = 12$.

If (12) has solutions then β is a unit with $\bar{\beta} = \zeta^a\beta$, where $\zeta^{2(a-1)} = -1$. Letting $\lambda^2 = \zeta^{-1}$(12) gives

$$(\beta - \lambda)(\beta + \lambda) = \beta^2 - \zeta^{-1} = 2(1 - \zeta)^{-1}.$$

As before if $n = 2^v$ this is impossible. For $n = 2^v m$, $m \geqslant 3$ odd we obtain $\beta - \lambda = \epsilon(1 + \zeta^{a-1})$ with ϵ a unit in $\mathbb{Q}(\lambda)$ and $\bar{\epsilon} = \lambda^b\epsilon$. Hence since the denominator is not zero

$$\beta = (\lambda^{-1} - \lambda^{b+1}\zeta^{-(a-1)})/(\zeta^a - \lambda^b\zeta^{-(a-1)}). \tag{17}$$

Substituting (17) in (12) gives, after some simplifying,

$$\lambda^b(1 + \zeta)(1 - \zeta^{1-a}((1 - \zeta)/(1 + \zeta))) + \zeta^{-b} + \zeta = 0.$$

Since the factor $(1 - \zeta^{1-a}((1 - \zeta)/(1 + \zeta)))$ cannot vanish for $n > 4$ we obtain that $\lambda^b \in \mathbb{Q}(\zeta)$. But then (17) implies that $\lambda \in \mathbb{Q}(\zeta)$, which is a contradiction. Thus (12) has no solutions and the proof of the theorem is complete.

Acknowledgment

The author would like to thank Professor V. Ennola and the referee for pointing out some errors in the original manuscript.

References

1. V. Ennola, Proof of a conjecture of Morris Newman, *J. Reine Angew. Math.* **264** (1973), 203–206.
2. V. Ennola, Solution of a cyclotomic diophantine equation, *J. Reine Angew. Math.* **273** (1975), 73–91.
3. L. J. Mordell, On a cyclotomic diophantine equation, *J. Math.* **42** (1963), 205–208.
4. M. Newman, Diophantine equations in cyclotomic fields, *J. Reine Angew. Math.* **265** (1974), 84–89.